

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-229392

(43)Date of publication of application : 25.08.1998

(51)Int.Cl.

H04L 9/16

G06K 17/00

G09C 1/00

H04L 9/32

H04M 15/00

(21)Application number : 09-029182

(71)Applicant : ROHM CO LTD

(22)Date of filing : 13.02.1997

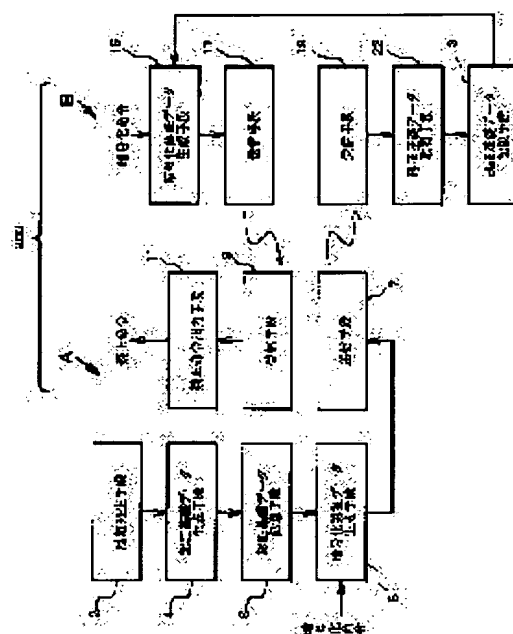
(72)Inventor : HIKITA JUNICHI  
IKUTO YOSHIHIRO  
CHIMURA SHIGEMI

## (54) AUTHENTICATION SYSTEM AND AUTHENTICATION METHOD

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an IC card which is difficult to be used by a person pretending to be a user.

**SOLUTION:** Ciphering authentication data are generated based on authentication fundamental data, including a random number part by using a ciphering rule, when a ciphering instruction is given by a ciphering authentication data generating means 5. The ciphering rule is varied according to the frequency of a given ciphering instruction. The ciphering authentication data are transmitted by a transmitting means 7. The ciphering authentication data transmitted from a second device B are received by a receiving means 9. A prohibiting instruction output means 11 judges whether or not the ciphering authentication data transmitted from the second device B match the ciphering authentication data generated, when the same frequency of the ciphering instruction is given to the ciphering authentication data-generating means of a first device A and outputs a prohibiting instruction to prohibit the transmission of the subject data to be transmitted, when a judging result is negative.



## LEGAL STATUS

[Date of request for examination]

19.11.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]





## 【特許請求の範囲】

【請求項1】第1の装置と第2の装置との間でデータ伝送を行なえるか否かの判断をする認証システムであって、

前記第1の装置および前記第2の装置間で伝送されるデータを暗号化する暗号化規則が単位伝送ごとに変化すること、

を特徴とする認証システム。

【請求項2】第1の装置と第2の装置との間で暗号化した認証データを伝送して、第1の装置と第2の装置との間における伝送対象データの伝送可否を判断する認証システムであって、

前記第1の装置および前記第2の装置間でやりとりされる暗号化された認証データが変化するように、前記認証データを暗号化する暗号化規則が単位伝送ごとに変化すること、

を特徴とする認証システム。

【請求項3】請求項2の認証システムにおいて、

前記第1の装置および前記第2の装置は、ともに、伝送回数に応じて、前記認証データを暗号化する暗号化規則が単位伝送ごとに変化するよう構成されており、

前記第1の装置は、前記第2の装置から送信されたデータが、伝送回数が同じ暗号化規則に基づいて暗号化されたデータと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力すること、

を特徴とする認証システム。

【請求項4】A) 第1の装置と第2の装置との間で伝送対象データを伝送する際の認証システムであって、

B) 前記第1の装置は、以下の手段を備え、

b1) 認証基礎データを記憶する認証基礎データ記憶手段、

b2) 暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段、

b3) 前記暗号化認証データを送信する送信手段、

b4) 前記第2の装置から送信された暗号化認証データを受信する受信手段、

C) 前記第2の装置は、以下の手段を備え、

c1) 前記第1の装置から送信された暗号化認証データを受信する受信手段、

c2) 前記暗号化認証データ生成手段における暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求める認証基礎データ取得手段、

c3) 得られた認証基礎データを記憶する認証基礎データ記憶手段、

c4) 前記第1の装置と同じ暗号化規則によって暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段、

ータ生成手段、

c5) 前記暗号化認証データを送信する送信手段、

D) 前記第1の装置は、さらに、前記第2の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する禁止命令出力手段を備えたこと、

を特徴とする認証システム。

【請求項5】請求項4の認証システムにおいて、

前記暗号化認証データ生成手段は、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則が変化するよう構成されていること、

を特徴とする認証システム。

【請求項6】請求項4または請求項5の認証システムにおいて、

乱数を発生させる乱数発生手段、

予め設定された設定データおよび前記乱数に基づいて、前記認証基礎データを前記認証基礎データ記憶手段に記憶させる認証基礎データ生成手段、

を備えたことを特徴とする認証システム。

【請求項7】請求項4～請求項6のいずれかの認証システムにおいて、

前記送信手段は、前記暗号化認証データを前記伝送対象データに付加させて送信し、

前記受信手段は、前記暗号化認証データが付加された前記伝送対象データを受信し、

前記認証基礎データ取得手段は、前記伝送対象データに付加された前記暗号化認証データを抽出して、認証基礎データを求めること、

を特徴とする認証システム。

【請求項8】請求項4～請求項7のいずれかの認証システムにおいて、

所定時間ごとに、前記暗号化認証データを送信すること、

を特徴とする認証システム。

【請求項9】請求項1～請求項8のいずれかの認証システムにおいて、

前記第1の装置は電話機であり、

前記第2の装置は、前記電話機用のICカードであり、前記電話機は、単位度数あたりの予め定められた通話可能時間が経過する都度、前記暗号化規則が変化するこ

と、

を特徴とする認証システム。

【請求項10】A) 第2の装置との間で伝送対象データを伝送する際の認証装置であって、

B) 以下の手段を備えたこと、

b1) 認証基礎データを記憶する認証基礎データ記憶手

段、

b2) 暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段

b3) 前記暗号化認証データを送信する送信手段、

b4) 前記第 2 の装置から送信された暗号化認証データを受信する受信手段、

b5) 前記第 1 の装置は、さらに、前記第 2 の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する禁止命令出力手段を備えたこと、  
を特徴とする認証装置。

【請求項 11】 A) 第 1 の装置との間で伝送対象データを伝送する際の認証データ作成装置であって、

B) 以下の手段を備えたこと、

1) 前記第 1 の装置から送信された暗号化認証データを受信する受信手段、

2) 前記第 1 の装置の暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求める認証基礎データ取得手段、

3) 得られた認証基礎データを記憶する認証基礎データ記憶手段、

4) 暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段

5) 前記暗号化認証データを送信する送信手段、  
を特徴とする認証データ作成装置。

【請求項 12】 2 つの装置間で、伝送対象データを伝送する際の認証方法であって、

与えられた暗号化命令回数に応じて暗号化規則を変化させて、双方側にて認証基礎データに基づいて暗号化認証データを生成し、生成した暗号化認証データをお互いに送受信し、同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データが一致するか否かを少なくとも一方側にて判断して、一致する場合にのみ、前記伝送対象データの伝送を可能とする認証方法において、  
前記他方側は、前記一方側から送られてきた暗号化認証データを前記暗号化規則に基づいて復号して、これを前記他方側の認証基礎データとすること、  
を特徴とする認証方法。

【請求項 13】 請求項 12 の認証方法において、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則を変化させること、  
を特徴とする認証方法。

【請求項 14】 請求項 13 の認証方法において、

前記認証基礎データは、乱数発生させた乱数部分を含んでいること、

を特徴とする認証方法。

【請求項 15】 請求項 12 ～ 請求項 14 のいずれかの認証方法において、

前記暗号化認証データは、前記伝送対象データに付加されて伝送されること、

を特徴とする認証方法。

10 【請求項 16】 請求項 12 ～ 請求項 14 のいずれかの認証方法において、

所定時間ごとに、前記暗号化認証データを送信すること、

を特徴とする認証方法。

【請求項 17】 請求項 12 ～ 請求項 14 のいずれかの認証方法において、

電話機用と電話機用 IC カードとの間の認証方法であって、単位度数あたりの予め定められた通話可能時間が経過する都度、前記認証を行なうこと、

を特徴とする認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、第 1 の装置と第 2 の装置との間で伝送対象データを伝送する際の認証に関するものであり、特に、その機密性の向上に関する。

【0002】

【従来技術】 スキー場のリフトや鉄道の自動改札、荷物の自動仕分け等に、IC カードを用いたデータ通信システムが提案されている。

30 【0003】 図 6 に、IC カードを用いたデータ通信システムのうち、非接触式 IC カードを用いた通信システムの構成を示す。このシステムは、質問器 240 (たとえば、スキー場のリフトのゲート内に搭載される) と非接触 IC カード 220 によって構成される。

【0004】 質問器 240 は、質問器側制御部 248 の制御により、発振回路 249 からの高周波搬送波をアンテナ 241 から送り出している。質問器 240 に対して非接触 IC カード 220 が接近すると、この高周波搬送波が非接触 IC カード 220 のアンテナ 224 によって  
40 受信される。電源生成回路 228 は、受信した高周波を直流電力に変換して、他の回路部分に供給する。このようにして、質問器 240 に近づくと、非接触 IC カード 220 が動作可能となる。

【0005】 また、質問器 240 から非接触 IC カード 220 に対する情報伝達は、前記高周波搬送波を変復調回路 233 において復調することにより行なわれる。カード側制御部 235 は、復調された情報に基づき、メモリ 237 の内容の書き換えや情報返信等の必要な処理を行う。

50 【0006】 一方、非接触 IC カード 220 から質問器

240に対しての情報伝達も行われる。非接触ICカード220側には、発振回路が設けられていないので、次の様にして、情報送信が行なわれる。質問器240の側から無変調の高周波搬送波を送り出しておき、非接触ICカード220側にて、変復調回路233により、共振回路222のインピーダンスを変化させる。質問器240は、このインピーダンス変化を、自己側の共振回路242のインピーダンス変化として、変復調回路246により検出して復調する。制御部248は、復調された情報を得て、必要な処理を行う。

【0007】非接触ICカード220が質問器240から遠ざかると、電力供給が無くなるので、非接触ICカード220の動作は停止する。なお、メモリ237は不揮発性メモリであるので、電力供給が無くなっても、記憶された情報は保持される。

【0008】以上のような非接触ICカード220のメモリ237に所定の度数を記憶させておき、使用度数に応じてメモリ237のデータを書換えることにより、プリペイドカードとして用いることができる。

【0009】質問器とICカードとの間の通信データは暗号化される。これによって、ICカードの代りとしてコンピュータを接続して、このコンピュータで正規のICカードになりますこと（以下「なりすまし」という）を防止している。

【0010】

【発明が解決しようとする課題】しかしながら、このような従来のICカードを用いた通信システムは、次のような問題点があった。上記のように、通信データを暗号化しても、暗号が解読されると、結局、前記なりすましが可能となる。

【0011】特に、前記ICカードを電話機に用いる場合、通話開始時における認証処理が解読され一旦通話状態となると、何時間でも通話状態とすることが可能となる。

【0012】この発明は、上記のような問題点を解決し、いわゆるなりすましが困難な認証システムおよび認証方法を提供することを目的とする。

【0013】さらに、電話機用の認証システムにおいて、通話開始時の認証処理が解読されても、その後、前記なりすましであるか否かの判断をすることができる認証システムを提供することを目的とする。

【0014】

【課題を解決するための手段】請求項1の認証システムにおいては、第1の装置と第2の装置との間でデータ伝送を行なえるか否かの判断をする認証システムであって、前記第1の装置および前記第2の装置間で伝送されるデータを暗号化する暗号化規則が単位伝送ごとに変化することを特徴とする。

【0015】請求項2の認証システムにおいては、第1の装置と第2の装置との間で暗号化した認証データを伝

送して、第1の装置と第2の装置との間における伝送対象データの伝送可否を判断する認証システムであって、前記第1の装置および前記第2の装置間でやりとりされる暗号化された認証データが変化するように、前記認証データを暗号化する暗号化規則が単位伝送ごとに変化することを特徴とする。

【0016】請求項3の認証システムにおいては、前記第1の装置および前記第2の装置は、ともに、伝送回数に応じて、前記認証データを暗号化する暗号化規則が単位伝送ごとに変化するよう構成されており、前記第1の装置は、前記第2の装置から送信されたデータが、伝送回数が同じ暗号化規則に基づいて暗号化されたデータと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力することを特徴とする。

【0017】請求項4の認証システムにおいては、

A) 第1の装置と第2の装置との間で伝送対象データを伝送する際の認証システムであって、

B) 前記第1の装置は、以下の手段を備え、

b1) 認証基礎データを記憶する認証基礎データ記憶手段、

b2) 暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段、

b3) 前記暗号化認証データを送信する送信手段、

b4) 前記第2の装置から送信された暗号化認証データを受信する受信手段、

C) 前記第2の装置は、以下の手段を備え、

c1) 前記第1の装置から送信された暗号化認証データを受信する受信手段、

c2) 前記暗号化認証データ生成手段における暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求める認証基礎データ取得手段、

c3) 得られた認証基礎データを記憶する認証基礎データ記憶手段、

c4) 前記第1の装置と同じ暗号化規則によって暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段、

c5) 前記暗号化認証データを送信する送信手段、

D) 前記第1の装置は、さらに、前記第2の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する禁止命令出力手段を備えたこと、を特徴とする認証システム。

【0018】請求項5の認証システムにおいては、前記暗号化認証データ生成手段は、暗号化された暗号化認証

データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則が変化するよう構成されていることを特徴とする。

【0019】請求項6の認証システムにおいては、乱数を発生させる乱数発生手段、予め設定された設定データおよび前記乱数に基づいて、前記認証基礎データを前記認証基礎データ記憶手段に記憶させる認証基礎データ生成手段を備えたことを特徴とする。

【0020】請求項7の認証システムにおいては、前記送信手段は、前記暗号化認証データを前記伝送対象データに付加させて送信し、前記受信手段は、前記暗号化認証データが付加された前記伝送対象データを受信し、前記認証基礎データ取得手段は、前記伝送対象データに付加された前記暗号化認証データを抽出して、認証基礎データを求めること、を特徴とする。

【0021】請求項8の認証システムにおいては、所定時間ごとに、前記暗号化認証データを送信することを特徴とする。

【0022】請求項9の認証システムにおいては、前記第1の装置は電話機であり、前記第2の装置は、前記電話機用のICカードであり、前記電話機は、単位度数あたりの予め定められた通話可能時間が経過する都度、前記暗号化規則が変化することを特徴とする。

【0023】請求項10の認証装置においては、  
A) 第2の装置との間で伝送対象データを伝送する際の認証装置であって、

B) 以下の手段を備えたこと、

b1) 認証基礎データを記憶する認証基礎データ記憶手段、

b2) 暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段

b3) 前記暗号化認証データを送信する送信手段、

b4) 前記第2の装置から送信された暗号化認証データを受信する受信手段、

b5) 前記第1の装置は、さらに、前記第2の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する禁止命令出力手段を備えたこと、を特徴とする。

【0024】請求項11の認証データ作成装置においては、

A) 第1の装置との間で伝送対象データを伝送する際の認証データ作成装置であって、

B) 以下の手段を備えたこと、

1) 前記第1の装置から送信された暗号化認証データを受信する受信手段、

2) 前記第1の装置の暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求める認証基礎データ取得手段、

3) 得られた認証基礎データを記憶する認証基礎データ記憶手段、

4) 暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する手段であって、与えられた暗号化命令回数に応じて前記暗号化規則が変化する暗号化認証データ生成手段

5) 前記暗号化認証データを送信する送信手段、を特徴とする。

【0025】請求項12の認証方法においては、2つの装置間で、伝送対象データを伝送する際の認証方法であって、与えられた暗号化命令回数に応じて暗号化規則を変化させて、双方側にて認証基礎データに基づいて暗号化認証データを生成し、生成した暗号化認証データをお互いに送受信し、同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データが一致するか否かを少なくとも一方側にて判断して、一致する場合にのみ、前記伝送対象データの伝送を可能とする認証方法において、前記他方側は、前記一方側から送られてきた暗号化認証データを前記暗号化規則に基づいて復号して、これを前記他方側の認証基礎データとすること、を特徴とする。

【0026】請求項13の認証方法においては、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則を変化させることを特徴とする。

【0027】請求項14の認証方法においては、前記認証基礎データは、乱数発生させた乱数部分を含んでいることを特徴とする。

【0028】請求項15の認証方法においては、前記暗号化認証データは、前記伝送対象データに付加されて伝送されることを特徴とする。

【0029】請求項16の認証方法においては、所定時間ごとに、前記暗号化認証データを送信することを特徴とする。

【0030】請求項17の認証方法においては、電話機用と電話機用ICカードとの間の認証方法であって、単位度数あたりの予め定められた通話可能時間が経過する都度、前記認証を行なうことを特徴とする。

【0031】

【発明の効果】請求項1の認証システムにおいては、前記第1の装置および前記第2の装置間で伝送されるデータを暗号化する暗号化規則が単位伝送ごとに変化する。したがって、いわゆるなりすましが困難な認証システムを提供することができる。

【0032】請求項2の認証システムにおいては、前記第1の装置および前記第2の装置間でやりとりされる暗号化された認証データが変化するよう、前記認証デー

データを暗号化する暗号化規則が単位伝送ごとに変化する。したがって、いわゆるなりすましが困難な認証システムを提供することができる。

【0033】請求項3の認証システムにおいては、前記第1の装置は、前記第2の装置から送信されたデータが、伝送回数が同じ暗号化規則に基づいて暗号化されたデータと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する。したがって、第1の装置と前記第2の装置との暗号化処理が異なる場合には、前記第1の装置と前記第2の装置との間の伝送を禁止することができる。また、暗号化規則の特定を伝送回数により行なうので、いわゆるなりすましがより困難となる。

【0034】請求項4の認証システムにおいては、前記第1の装置は、暗号化命令が与えられると、前記認証基礎データに基づいて与えられた暗号化命令回数に応じた暗号化認証データを生成し、これを送信する。前記第2の装置は、前記第1の装置から送信された暗号化認証データを受信し、前記暗号化認証データ生成手段における暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求め、得られた認証基礎データを記憶する。そして、前記第1の装置と同じく、前記認証基礎データに基づいて与えられた暗号化命令回数に応じた暗号化認証データを生成し、これを送信する。前記第1の装置は、前記第2の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する。

【0035】したがって、前記第1の装置に記憶されている認証基礎データを前記第2の装置に伝送することができる。そして、前記第2の装置における暗号化認証データが異なる生成処理によって行なわれた場合には、前記第1の装置と前記第2の装置との間の伝送を禁止することができる。これにより、いわゆるなりすましが困難な認証システムを提供することができる。

【0036】請求項5の認証システムにおいては、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則が変化する。したがって、多重処理の回数を制御するだけで暗号化命令回数に応じた暗号化認証データを生成することができる。

【0037】請求項6の認証システムにおいては、前記認証基礎データ生成手段は、予め設定された設定データおよび前記乱数に基づいて、前記認証基礎データを前記認証基礎データ記憶手段に記憶させる。したがって、前記認証基礎データが固定化されることがない。これにより、いわゆるなりすましがより困難となる。

【0038】請求項7の認証システムにおいては、前記

送信手段は、前記暗号化認証データを前記伝送対象データに付加させて送信し、前記受信手段は、前記暗号化認証データが付加された前記伝送対象データを受信し、前記認証基礎データ取得手段は、前記伝送対象データに付加された前記暗号化認証データを抽出して、認証基礎データを求める。したがって、前記暗号化認証データを伝送するために、前記伝送対象データと別途伝送する必要がない。

【0039】請求項8の認証システムにおいては、所定時間ごとに、前記暗号化認証データを送信する。したがって、一旦認証したあとも、所定時間ごとに前記認証処理をすることができる。

【0040】請求項9の認証システムにおいては、前記第1の装置は電話機であり、前記第2の装置は、前記電話機用のICカードであり、前記電話機は、単位度数あたりの予め定められた通話可能時間が経過する都度、前記暗号化規則が変化する。したがって、単位度数あたりの予め定められた通話可能時間経過毎に、前記認証処理が行なわれる。これにより、通話開始時だけでなく、単位度数の通話時間経過ごとに前記照合をすることができる。

【0041】請求項10の認証装置においては、暗号化命令が与えられると、前記認証基礎データに基づいて与えられた暗号化命令回数に応じた暗号化認証データを生成し、これを送信する。そして、前記第2の装置から送信された暗号化認証データが、自己の暗号化認証データ生成手段に同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する。したがって、前記第2の装置が行なう生成処理が異なる生成処理である場合には、前記第2の装置との間の伝送を禁止することができる。

【0042】請求項11の認証データ作成装置においては、前記第1の装置から送信された暗号化認証データを受信する。そして、暗号化命令が与えられると、前記認証基礎データに基づいて与えられた暗号化命令回数に応じた暗号化認証データを生成し、これを送信する。これにより、前記第2の装置にて、前記第1の装置の認証基礎データを受け取ることができる。また、前記第1の装置にて、前記第2の装置における暗号化認証データを検証することができる。

【0043】請求項12の認証方法においては、与えられた暗号化命令回数に応じて暗号化規則を変化させて、双方側にて認証基礎データに基づいて暗号化認証データを生成し、生成した暗号化認証データをお互いに送受信し、同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データが一致するか否かを少なくとも一方側にて判断して、一致する場合にのみ、前記伝送対象データの伝送を可能とする。さらに、前記一方側から送ら



れてきた暗号化認証データを、他方側は前記暗号化規則に基づいて復号して、これを前記他方側の認証基礎データとする。したがって、他方側には、認証基礎データを記憶していなくとも、一方側と他方側にて生成された暗号化認証データが一致しない場合には前記伝送を禁止することができる。

【0044】請求項13の認証方法においては、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則を変化させる。したがって、生成回数に応じて異なる暗号化認証データを生成することができる。

【0045】請求項14の認証方法においては、前記認証基礎データは、乱数発生させた乱数部分を含んでい。したがって、前記認証基礎データが固定化されることがない。これにより、いわゆるなりすましがより困難となる。

【0046】請求項15の認証方法においては、前記暗号化認証データは、前記伝送対象データに付加されて伝送される。したがって、前記伝送対象データを伝送するだけで前記暗号化認証データを伝送することができる。

【0047】請求項16の認証方法においては、所定時間ごとに、前記暗号化認証データを送信する。したがって、一旦認証したあとも、所定時間ごとに前記認証処理をすることができる。

【0048】請求項17の認証方法においては、電話機用と電話機用ICカードとの間の認証方法であって、単位度数あたりの予め定められた通話可能時間が経過する都度、前記認証を行なう。したがって、通話開始時だけでなく、通話中にも前記照合をすることができる。

【0049】

【発明の実施の形態】図面を用いて、本発明にかかる認証システム200の機能ブロック図について説明する。図1に示す認証システム200は、第1の装置Aと第2の装置Bとの間で伝送対象データを伝送する際の認証を行なう認証システムである。

【0050】第1の装置Aは、乱数発生手段2、認証基礎データ生成手段4、認証基礎データ記憶手段3、暗号化認証データ生成手段5、送信手段7、受信手段9および禁止命令出力手段11を備えている。乱数発生手段2は乱数を発生させる。認証基礎データ生成手段4は、予め設定された設定データおよび前記乱数に基づいて、前記認証基礎データを生成して、認証基礎データ記憶手段3に記憶させる。

【0051】暗号化認証データ生成手段5は、暗号化命令が与えられると、暗号化規則を用いて前記認証基礎データに基づいて暗号化認証データを生成する。この暗号化規則は、与えられた暗号化命令回数に応じて変化する。本実施形態においては、暗号化された暗号化認証データの多重処理回数を変更することにより、与えられた暗号化命令回数に応じて前記暗号化規則が変化するよう

にした。送信手段7は、前記暗号化認証データを送信する。

【0052】一方、第2の装置Bは、受信手段19、認証基礎データ取得手段22、認証基礎データ記憶手段13、暗号化認証データ生成手段15、および送信手段17を備えている。

【0053】受信手段19は、第1の装置Aから送信された暗号化認証データを受信する。認証基礎データ取得手段22は、第1の装置Aの暗号化認証データ生成手段5における暗号化規則に基づいて、前記暗号化認証データから認証基礎データを求める。認証基礎データ記憶手段13は、得られた認証基礎データを記憶する。暗号化認証データ生成手段15は、暗号化認証データ生成手段5と同じ暗号化規則によって暗号化認証データを生成する。なお、第1の装置と同様に、与えられた暗号化命令回数に応じて前記暗号化規則が変化する。送信手段17は、この暗号化認証データを送信する。

【0054】第1の装置Aの受信手段9は、第2の装置Bから送信された暗号化認証データを受信する。禁止命令出力手段11は、第2の装置Bから送信された暗号化認証データが、第1の装置Aの暗号化認証データ生成手段と同じ回数暗号化命令を与えたとした場合に生成される暗号化認証データと一致するか否かを判断して、判断結果が否定的である場合には、前記伝送対象データの伝送を禁止する禁止命令を出力する。

【0055】したがって、第1の装置Aに記憶されている認証基礎データを第2の装置Bに伝送することができる。そして、第2の装置Bにおける暗号化認証データが異なる生成処理によって行なわれた場合には、第1の装置Aと第2の装置Bとの間の伝送を禁止することができる。これにより、いわゆるなりすましが困難な認証システムを提供することができる。

【0056】つぎに、第1の装置Aのハードウェア構成について、図2を用いて説明する。

【0057】第1の装置Aは、主制御部41、乱数発生器43、乱数ラッチ45、パスワード記憶部47、認証基礎データラッチ49、演算器51、デコード53、ROM55、シフトレジスタ57、比較用ラッチ59、比較器61および伝送回路63を有する。

【0058】主制御部41は、後述するように各部の制御を行なう。乱数発生器43は、主制御部41から乱数発生命令が与えられると、64ビットの乱数を発生させる。乱数ラッチ45は、乱数発生器43にて発生した乱数を保持する。

【0059】パスワード記憶部47は、3つのパスワードを記憶する。この場合、パスワード1は、64ビットの第1の装置のハードウェア製造者のパスワードであり、パスワード2は、32ビットの第1の装置Aの運用者のパスワードであり、パスワード3は、32ビットの第1の装置のソフトウェア設計者のパスワードである。

【0060】認証基礎データラッチ49は、パスワード記憶部47および乱数ラッチ45から与えられた128ビットのデータを保持する。本実施形態においては、認証基礎データラッチ49に保持されるデータが認証基礎データに該当する。

【0061】比較用ラッチ59には、初期状態では、128ビットの初期値が保持されている。本実施形態においては初期値として、「00・・・00」（128ビット）を保持させた。

【0062】演算器51は、認証基礎データラッチ49と比較用ラッチ59とに保持されているデータについて所定の演算を行なう演算器である。具体的には各々のデータの排他的論理和演算を行なう。デコーダ53は、128ビットのデータが与えられると、これを16ビットのデータにデコードする。ROM55は、16ビットのアドレスについて、128ビットのデータ長のデータを記憶しており、16ビットのデータを所定の128ビットのデータにデータ変換する。これにより、暗号化処理がなされる。

【0063】比較器61は、シフトレジスタ57のデータと比較用ラッチ59のデータを比較して、主制御部41に比較結果を出力する。伝送回路63は、第2の装置Bとのデータ伝送を行なう。

【0064】なお、シフトレジスタ57は、ROM55または比較器61への入出力は128ビットがパラレル処理され、伝送回路63との入出力は1ビットずつシリアル処理される。

【0065】つぎに、第2の装置1のハードウェア構成について、図3を用いて説明する。

【0066】第2の装置Bは、主制御部81、乱数ラッチ85、パスワード記憶部87、認証基礎データラッチ89、演算器91、デコーダ93、ROM95、シフトレジスタ97、比較用ラッチ99、伝送回路103、ROM105、エンコーダ107および乱数デコーダ109を有する。

【0067】乱数ラッチ85、パスワード記憶部87、認証基礎データラッチ89、演算器91、デコーダ93、ROM95、シフトレジスタ97、比較用ラッチ99、伝送回路103については、それぞれ乱数ラッチ45、パスワード記憶部47、認証基礎データラッチ49、演算器51、デコーダ53、ROM55、シフトレジスタ57、比較用ラッチ59、伝送回路63と同じであるので説明は省略する。

【0068】ROM105は、ROM55とは、逆方向の処理（復号化）を行なうROMであり、128ビットのアドレスについて、16ビットのデータ長のデータを記憶しており、128ビットのデータを所定の16ビットのデータに復号化する。

【0069】エンコーダ107は、デコーダ53とは逆の処理を行なう。すなわち、16ビットのデータが与え

られると、これを所定の128ビットのデータにエンコードする。乱数デコーダ109は、この128ビットのデータからパスワード記憶部87に記憶されている64ビットのデータを用いて、残り64ビットのデータを取り出す。取り出された64ビットのデータは、乱数ラッチ85に保持される。

【0070】すなわち、第2の装置Bは、第1の装置Aとほぼ同じ構成であるが、乱数発生器43および比較器61を有せず、一方、ROM105、エンコーダ107、乱数デコーダ109を有する。

【0071】つぎに、認証処理について説明する。まず、主制御部41は、シフトレジスタ57に、伝送対象のデータの先頭8ビットが与えられると、これを検知し、乱数発生器43に乱数発生命令を与える。乱数発生器43はこれを受けて、64ビットの乱数を発生させる。ここで、この64ビットの乱数を値aとする。ここで、乱数発生器43にて発生した乱数は乱数ラッチ45にて保持される。

【0072】認証基礎データラッチ49には、パスワード記憶部47および乱数ラッチ45から与えられた128ビットのデータが保持される。

【0073】ここで、認証基礎データラッチ49に保持されるデータをデータAとする。また、比較用ラッチ59には、初期状態では、初期値「00・・・00」（128ビット）が保持されているので、演算器51にて排他的論理和演算が行なわれる。デコーダ53は、128ビットのデータを16ビットのデータにデコードし、ROM55は、与えられた16ビットのデータを128ビットのデータにデータ変換する。シフトレジスタ57に、この128ビットのデータが与えられる。シフトレジスタ57に与えられるデータをデータA'とする。このデータA'が伝送対象のデータの先頭に付加されて伝送回路63から送信される。

【0074】図4Aに認証基礎データラッチ49、比較用ラッチ59、シフトレジスタ57に保持されるデータを示す。このように、第1回目の暗号化認証データの送信時には、認証基礎データラッチ49にデータA、比較用ラッチ59にデータ0、シフトレジスタ57にデータA'が保持される。

【0075】つぎに、主制御部41は、比較用ラッチ59に取込み命令を出力する。比較用ラッチ59の入力には、ROM55からのデータすなわちデータA'が与えられているので、比較用ラッチ59は取込み命令を受けて、データをA'保持する。比較用ラッチ59にデータA'が保持されると、演算器51、デコーダ53、ROM55によって、比較用ラッチ59の入力には、ROM55からのデータすなわちデータ（AeorA'）'が与えられる。なお、AeorA'とは、データAとデータA'との排他的論理和演算を表す。主制御部41は、再度、比較用ラッチ59に取込み命令を出力する。これに

より、比較用ラッチ59にはデータ(AeorA')'が保持される。

【0076】このように、第1の装置Aにおいては、図4Bに示すように、第2の装置Bに送信した後、比較用ラッチ59に伝送回路63に与えた暗号化認証データを、さらに暗号化したデータを保持している。

【0077】一方、図3に示す第2の装置Bは、伝送回路103で、データA'が付加された伝送対象のデータを受信する。データA'が付加された伝送対象のデータから先頭の128ビットのデータがROM105に与えられ、128ビットのデータを16ビットのデータにデータ変換する。エンコーダ107は、与えられた16ビットのデータを128ビットのデータにエンコードする。乱数デコーダ109は128ビットのデータから、パスワード記憶部87に記憶されている64ビットのデータを用いて、残り64ビットのデータを取り出す。取り出された64ビットのデータは、乱数ラッチ85に保持される。

【0078】このようにして、第1の装置Aで発生させた乱数aを第2の装置Bの乱数ラッチ85に伝送することができる。

【0079】つぎに、伝送回路103の受信信号を受けて、主制御部81は認証基礎データラッチ89に取込み命令を与える。これにより、認証基礎データラッチ89に乱数ラッチ85とパスワード記憶部87に保持されたデータが取込まれる。この場合、図5Aに示すように、シフトレジスタ97に、データA'、認証基礎データラッチ89にデータA、比較用ラッチ99にデータ0が保持される。

【0080】つぎに、主制御部81は、シフトレジスタ97に伝送対象のデータの先頭8ビットが与えられると、これを検知し、認証基礎データラッチ89に取込み命令を与える。これにより、認証基礎データラッチ89には、パスワード記憶部87および乱数ラッチ85から与えられた128ビットのデータが保持される。

【0081】ここで、認証基礎データラッチ89には、第1の装置と同様に、データAが保持される。なぜなら、乱数ラッチ85に保持されたデータおよびパスワード記憶部87に記憶されたパスワードが同じだからである。また、比較用ラッチ99には、初期状態では、第1の装置Aと同様に、初期値「00...00」(128ビット)が保持されている。演算器91は、認証基礎データラッチ89と比較用ラッチ99に保持されたデータの排他的論理和演算を行なう。

【0082】デコーダ93は、128ビットのデータを16ビットのデータにデコードし、ROM95は、与えられた16ビットのデータを128ビットのデータにデータ変換する。シフトレジスタ97に、この128ビットのデータが与えられる。この場合、データ(AeorA')'がシフトレジスタ97に与えられる。制御部8

1から伝送命令が与えられると、このデータ(AeorA')'が伝送対象のデータの先頭に第2回目の暗号化認証データが付加されて伝送回路103から送信される。

【0083】図5Bに、認証基礎データラッチ89、比較用ラッチ99、シフトレジスタ97に保持されるデータを示す。このように、第2の装置の第1回目の暗号化認証データの送信時には、認証基礎データラッチ49にデータA、比較用ラッチ59にデータA'シフトレジスタ97にデータ(AeorA')'が保持される。

【0084】つぎに、主制御部81は、比較用ラッチ99に取込み命令を出力する。比較用ラッチ99の入力には、ROM95からのデータ、すなわちデータ(AeorA')'が与えられているので、比較用ラッチ99は取込み命令を受けて、データ(AeorA')'を保持する。比較用ラッチ99にデータ(AeorA')'が保持されると、演算器91、デコーダ93、ROM95によって、比較用ラッチ99の入力には、ROM95からのデータ、すなわちデータ(Aeor(AeorA')')'が与えられる。主制御部81は、再度、比較用ラッチ99に取込み命令を出力する。これにより、比較用ラッチ99にはデータ(Aeor(AeorA')')'が保持される。

【0085】このように、第2の装置Bにおいても、図5Cに示すように、第1の装置に送信した後、比較用ラッチ99に、演算器91、デコーダ93、ROM95によって、暗号化したデータを保持している。これは、以下の様な理由による。本実施形態においては、第1の装置Aから第2の装置Bへ、または、第2の装置Bから第1の装置Aへと照合用データを転送する都度、前記暗号化処理を行なっている。したがって、第1の装置Aと第2の装置Bとでお互いに行なっている処理を一致させる必要があるからである。

【0086】第1の装置Aは、伝送回路63で、データ(AeorA')'が付加された伝送対象のデータを受信する。データ(AeorA')'が付加された伝送対象のデータからシフトレジスタ57に与えられると、主制御部41は、シフトレジスタ57に出力命令を与える。これにより、先頭の128ビットのデータが、比較器61に与えられる。また、主制御部41は、比較器61に照合命令を与える。これにより、比較器61は、比較用ラッチ59に保持されたデータとシフトレジスタ57から与えられたデータを比較する。この場合、第1の装置Aと第2の装置Bとが正規の装置であるので、比較器61は一致信号を主制御部41に与える。もし、第2の装置Bがなりすましの装置である場合には、比較用ラッチ59に保持されたデータとシフトレジスタ57から与えられたデータが一致しないので、この場合は主制御部41は、伝送禁止命令を出力する。これにより、なりすましを確実に防止することができる。

【0087】以後、同様にして、第1の装置Aからの第3回目の暗号化認証データの送信が行なわれ、第2の装置Bは送信された暗号化認証データが比較用ラッチ59に記憶されたデータと一致するか否かが判断される。

【0088】このようにして、暗号化認証データを順次変更して送ることにより、確実になりすましを防止することができる。

【0089】また、本実施形態においては、伝送対象データの先頭に128ビットのデータを付加して、伝送しているので、暗号化認証データが付加された伝送対象データとして伝送データを見てみると、伝送対象データも結果的に暗号化されているので、命令（コード）を知られることも防止できる。なお、このように、暗号化認証データを付加して伝送するのではなく、暗号化認証データだけを伝送して、前記照合を行なうようにしてもよい。

【0090】なお、本実施形態においては、第2の装置から送信された暗号化認証データはそのままとし、比較用ラッチ59に、演算器51、デコーダ53、ROM55によって再度暗号化した暗号化認証データを記憶させることにより、一致しているか否かを判断するようにした。これにより、第1の装置Aには、演算器51、デコーダ53、ROM55の逆の処理を行なう回路が不要となる。

【0091】しかし、かかる方法に限定されず、第2の装置から送信された暗号化認証データを演算器51、デコーダ53、ROM55の逆の処理を行なう回路にて、復号化して比較するようにしてもよい。さらに、第1の装置A側では、演算器51、デコーダ53、ROM55の逆の処理全部ではなく、一部だけ行ない、第2の装置から送信された暗号化認証データをこれと一致する処理を行なう様にしてもよい。

【0092】本実施形態においては、本発明をICカード（第2の装置）とそのリードライタ（第1の装置）に用いた場合について説明したが、第1の装置と第2装置間でデータを伝送させるシステムであれば、ICカード以外のどの様な装置でも用いることができる。

【0093】また、非接触式ICカードに限らず、接触式ICカードにも適用することができる。

【0094】なお、本実施形態においては、前回と異なる暗号化データの生成については、入力データをフィードバックすることによりこれを実現するようにしたが、入力データを所定の規則に基づいて、値を替えるようにしてもよい。また入力データを変更することなく、暗号化のアルゴリズムを変更するようにしてもよい。

【0095】なお、本実施形態においては、伝送対象データの先頭の8ビット分のデータガシフトレジスタに与えられると、前記暗号化認証データを伝送対象データに付加して伝送している。しかし、伝送対象データの伝送とは無関係に、所定時間をタイマで計測して、所定時間

ごとに、前記暗号化認証データだけを伝送するようにしてもよい。

【0096】また、各伝送対象データごとに前記暗号化認証データを変更しているが、複数伝送対象データごとに変更するようにしてもよい。

【0097】また、8ビットを検出すると、暗号化認証データの生成を行なうようにしているが、これは、上記暗号化認証データの生成処理に要する時間で決定すればよい。

【0098】また、暗号化認証データおよび伝送対象データのビット長については、これらに限定されるものではない。

【0099】なお、本実施形態においては、暗号化処理を第1の装置と第2の装置とで、お互いに1回ずつ多重化していくことにより、暗号化命令の回数を伝送することなく、照合する際の暗号化命令の回数を決定している。これにより、どの様にして暗号化されているかを解析しにくくなる。

【0100】しかし、これに限定されず、暗号化命令の回数を伝送するようにしてもよい。

【0101】第1の装置で乱数部分の値を部分的に決定し、第2の装置で残りの部分の値を決定し、これを統合して、乱数ラッチ45、乱数ラッチ85に記憶するようにしてもよい。これにより、より機密性を高くすることができる。

【0102】なお、一部をソフトウェアで実現するようにしてもよい。

【0103】なお、本明細書において、「与えられた暗号化命令回数に応じて前記暗号化規則が変化する」とは、実施形態に示すように、暗号化の多重度を変更することにより、これを実現する場合はもちろん、複数の暗号化規則を記憶しておき、暗号化命令回数に応じて、これを切替えるものも含む。また、暗号化の多重度とは、第1の装置Aでは、演算器51、デコーダ53、ROM55によって暗号化した暗号化処理回数を意味し、第2の装置Bでは、演算器91、デコーダ93、ROM95によって暗号化した暗号化処理回数に該当する。

【0104】また、本発明にかかる認証システムを電話機とそのICカードとの間の認証に用いることもできる。この場合、電話機側の制御部41には、1度数あたりの予め定められた通話可能時間が経過する都度、伝送対象のデータである度数削除命令が与えられることとなるので、ROM55等による暗号化処理を行ない、伝送回路63から、ICカードに対して、暗号化認証データを送るようにすればよい。これにより、1度数あたりの予め定められた通話可能時間が経過する都度、前記照合をすることができる。なお、1度数あたりの予め定められた通話可能時間が経過する都度ではなく、数度数を単位度数として予め定められた通話可能時間が経過する都度前記暗号化認証データを送るようにしてもよい。

【0105】なお、電話機に用いる場合には、ＩＣカードに記憶されている残度数を最初に読み出しておき、この残度数の範囲内であれば通話可能とするとともにＩＣカードとの間では伝送対象データを伝送せずに、通話終了時に残度数をＩＣカード側に送信し、ＩＣカードの残度数を書換えることも考えられる。この場合には、所定時間経過ごとに、前記暗号化認証データだけを送るようにしてもよい。具体的には、タイマで経過時間を計測しておき、所定時間経過すると、制御部４１に暗号化命令を与え、ROM５５等による暗号化処理を行なうようにすればよい。

【0106】また、本実施形態においては、認証を行なう為の暗号化認証データを伝送対象のデータの先頭に付加して送信し、受信側で暗号化認証データを抽出するようにした。しかしこれに限定されず、伝送対象データを所定の内容としておき、伝送対象のデータを所定の暗号化規則にて暗号化して送信し、受信側にて対応する復号処理を行ない、伝送された伝送対象データが前記所定の内容であるかを判断するようにしてもよい。すなわち、認証データとは、伝送対象データとは別に伝送される場合はもちろん、伝送対象データそれ自体を間接的に認証データとして用いる場合も含む。

【0107】また、「暗号化規則が単位伝送ごとに変化する」とは、送信側から受信側に伝送される都度、すなわち、伝送１回毎に暗号化規則が変化する場合はもちろん、所定伝送回数ごとに暗号化規則が変化する場合を含む。

【図面の簡単な説明】

【図１】本発明にかかる本発明にかかる認証システム２００の全体構成図である。

【図２】第１の装置Ａのハードウェア構成を示す図である。

【図３】第２の装置Ｂのハードウェア構成を示す図である。

\*

【図４】

A 第1発信時		B 準備時		C 受信時	
ラッチ49	A	ラッチ49	A	ラッチ49	A
ラッチ59	O	ラッチ59	(AeorA')'	ラッチ59	(AeorA')'
シフトレジスタ	A'	シフトレジスタ	—	シフトレジスタ	(AeorA')'

\* 【図４】第１の装置Ａの認証基礎データラッチ、比較用ラッチ、シフトレジスタに保持されるデータの遷移を示す図である。

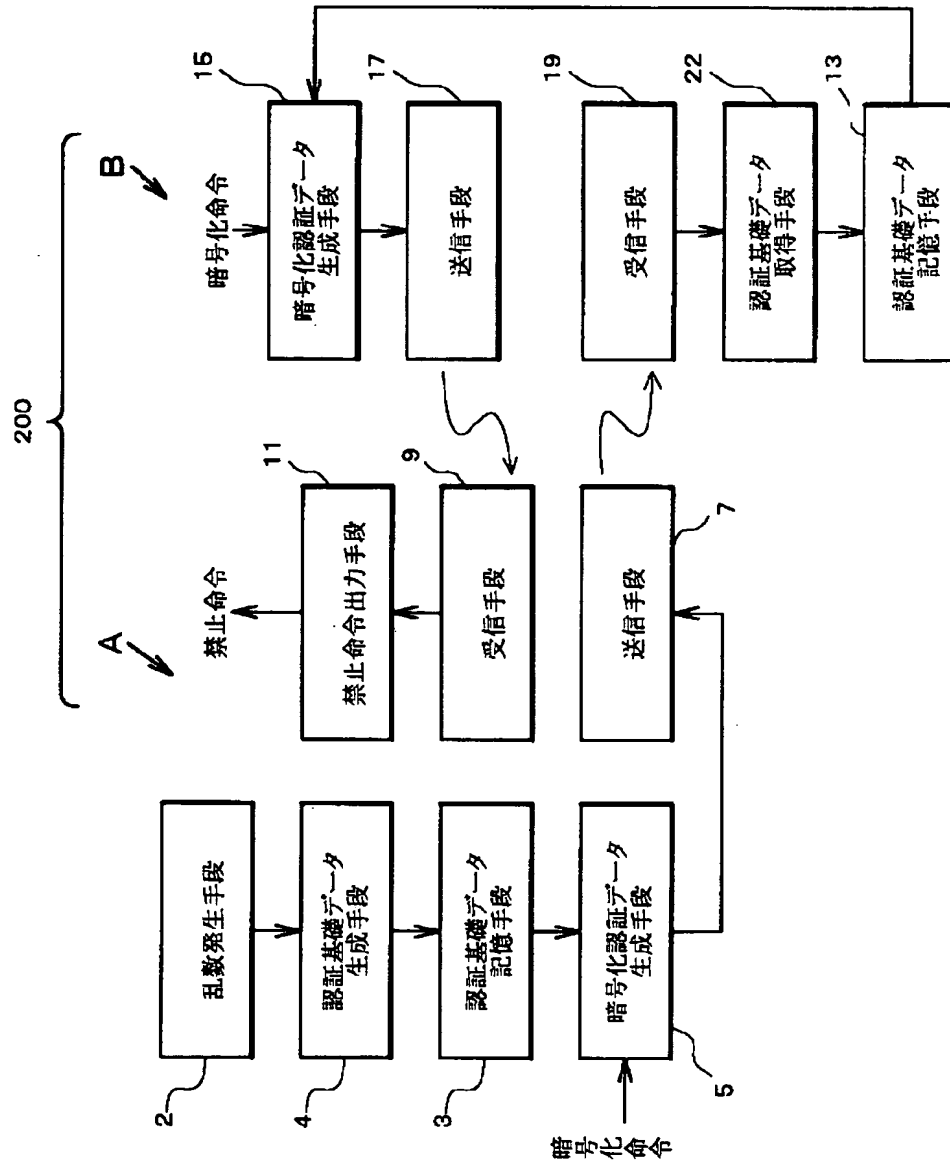
【図５】第２の装置Ｂの認証基礎データラッチ、比較用ラッチ、シフトレジスタに保持されるデータの遷移を示す図である。

【図６】従来のＩＣカード３００を示す図である。

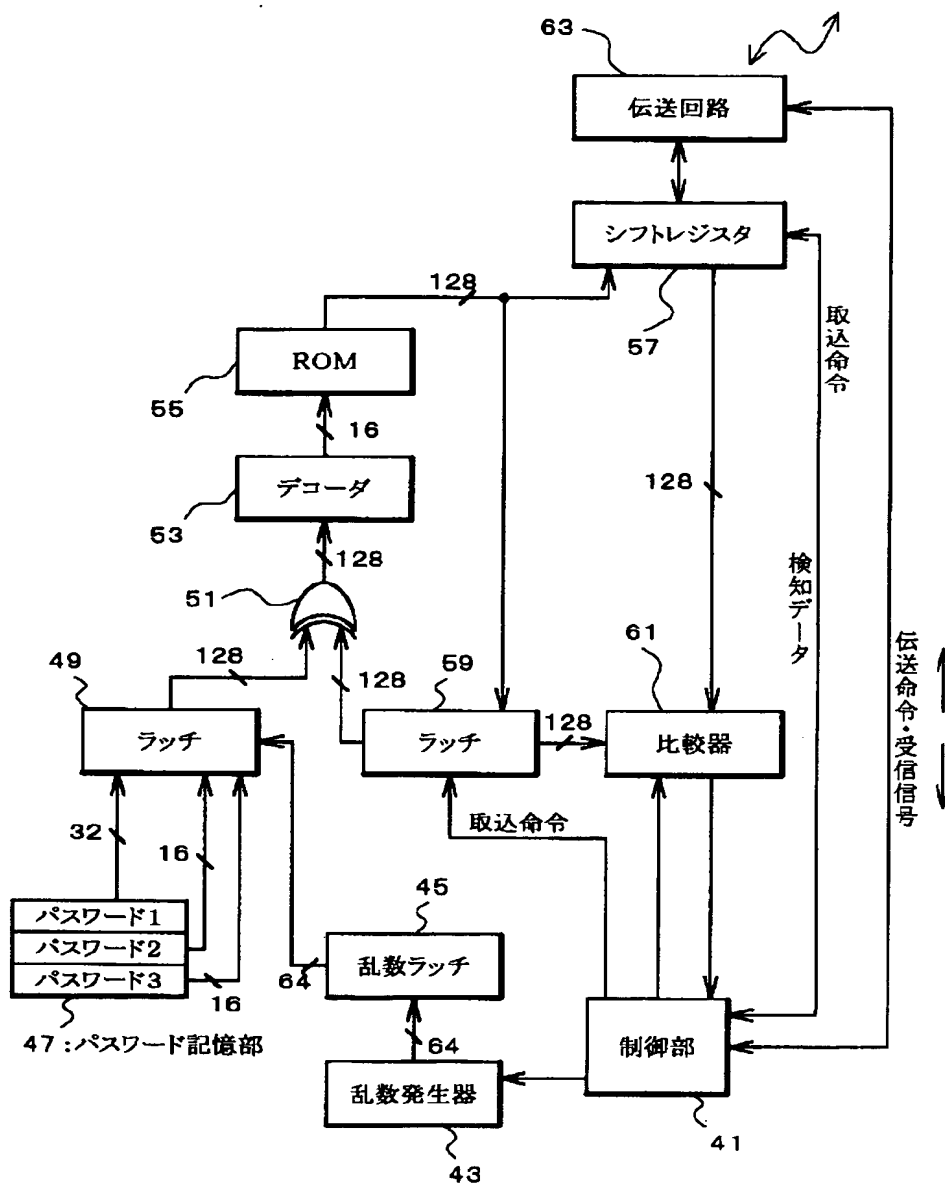
【符号の説明】

41・・・・・・主制御部  
 43・・・・・・乱数発生器  
 45・・・・・・乱数ラッチ  
 47・・・・・・パスワード記憶部  
 49・・・・・・認証基礎データラッチ  
 51・・・・・・演算器  
 53・・・・・・デコーダ  
 55・・・・・・ROM  
 57・・・・・・シフトレジスタ  
 59・・・・・・比較用ラッチ  
 61・・・・・・比較器  
 63・・・・・・伝送回路  
 81・・・・・・主制御部  
 85・・・・・・乱数ラッチ  
 87・・・・・・パスワード記憶部  
 89・・・・・・認証基礎データラッチ  
 91・・・・・・演算器  
 93・・・・・・デコーダ  
 95・・・・・・ROM  
 97・・・・・・シフトレジスタ  
 99・・・・・・比較用ラッチ  
 103・・・・・・伝送回路  
 105・・・・・・ROM  
 107・・・・・・エンコーダ  
 109・・・・・・乱数デコーダ

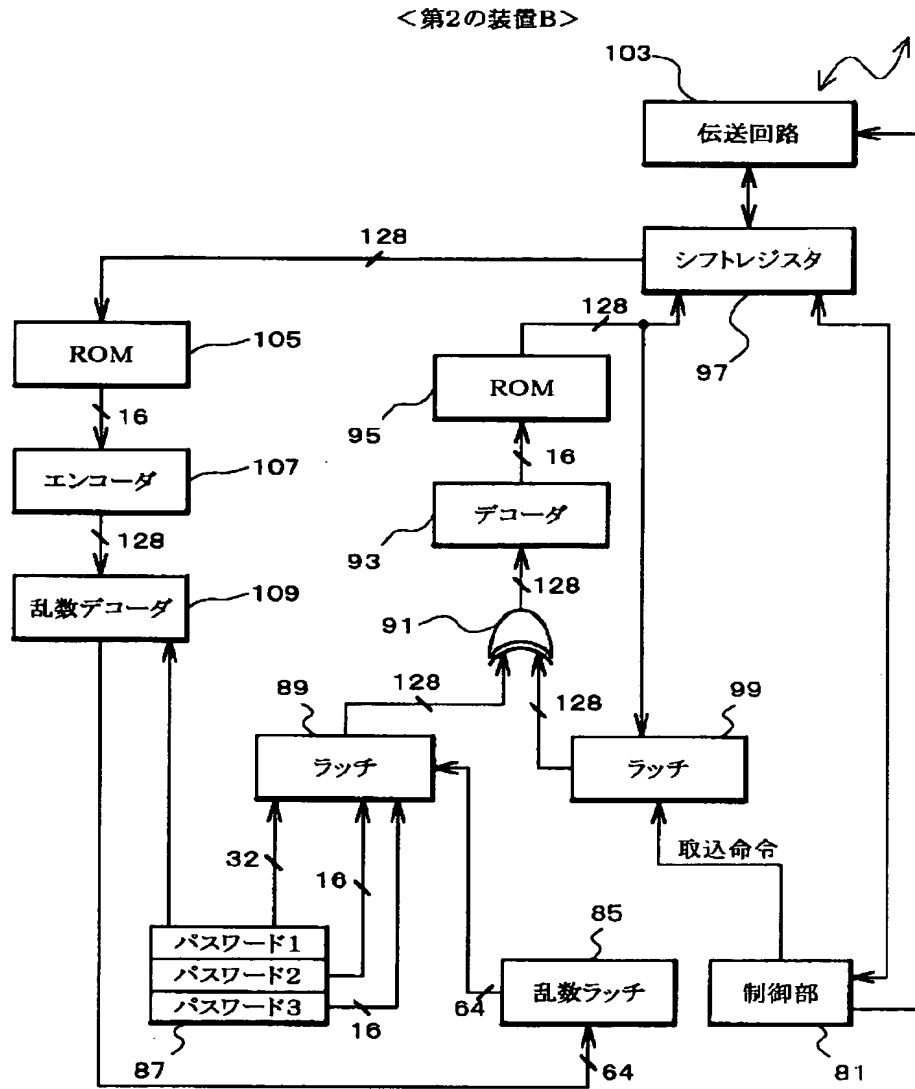
【図1】



＜第1の装置A＞



【図3】



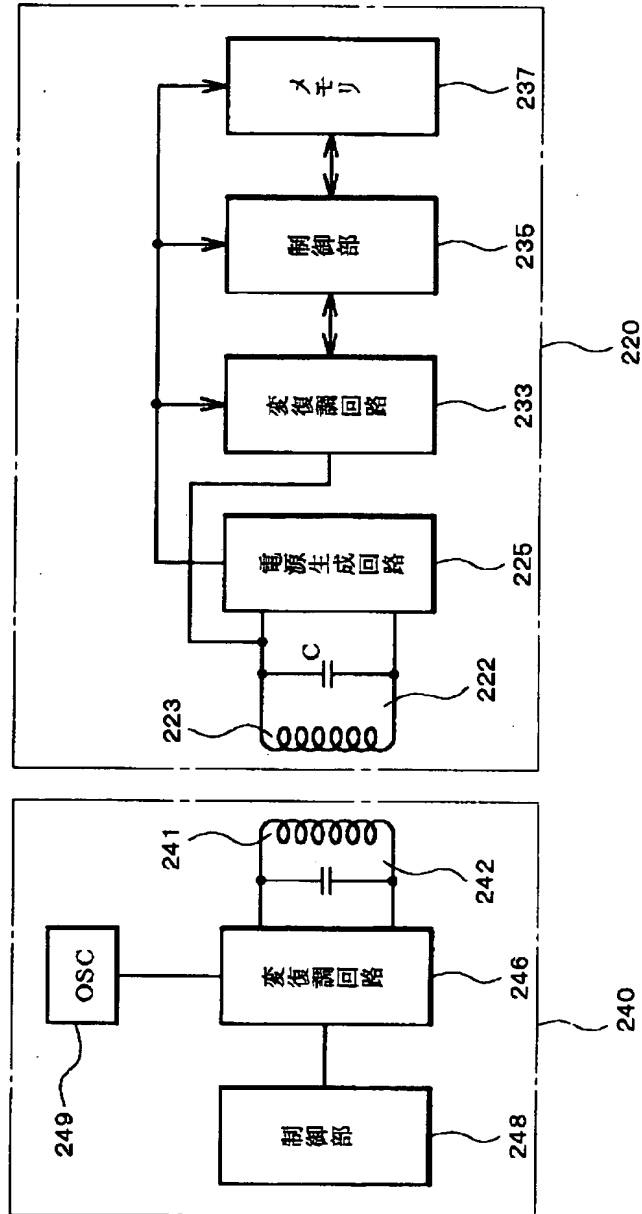


【図 5】

A 受信時		B 発信時		C 準備時	
ラッチ89	A	ラッチ89	A	ラッチ89	A
ラッチ99	0	ラッチ99	—	ラッチ99	$(A \oplus A')'$
シフト レジスタ	$A'$	シフト レジスタ	$(A \oplus A')'$	シフト レジスタ	—

【図 6】

&lt;従来技術&gt;



フロントページの続き

(51) Int. Cl.<sup>6</sup>

識別記号

F I  
H 0 4 L 9/00

6 7 3 E